UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/092,972	03/08/2002	Scott A. Vanstone	00001-0436	1483

7590 03/29/2006

Orange & Chari
66 Wellington St. W., Suite 4900
P.O. Box 190
Toronto, ON M5K 1H6
CANADA

EXAMINER	
SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 03/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/092,972	VANSTONE ET AL.	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 March 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *06/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responding to the Application received on 03/08/2002.

2. Claims 1-19 are pending.

Claim Objections

3. Claim 1 is objected to because of the following informalities: $g^{(y)}$ in step iii) of claim 1 (It should be g(y)). Appropriate correction is required.

4. In step IV) of claim 1, the term "for" in the part of the step IV from "said session key K also being constructible by said first correspondent A "for" (should be "from") information made public by B and ..." Appropriate correction is required to all similar mistakes in all claims.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 1 recites the limitation "said second" in step VI). There is insufficient antecedent basis for this limitation in the claim.

Double Patenting

7. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

8. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory

double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

9. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

10. Claims 1-18 in this application (10/092972), hereinafter "972, rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-16 of prior U.S. Patent No. 6487661B2, hereinafter "661. Although the conflicting claims are not identical, they are not patentably distinct from each other because the Exemplary Claim 1 in "661 recites "the method of authenticating ... in a public key data communication system ... over a communication channel" and the Exemplary Claim 1 in "972 does not have such limitation. However, it would be obvious at the time of the invention was made for one having ordinary skill in the art to realize that the method of authenticating in "972 is also in a public key data communication system since the method including the utilization of the public and private key exchange.

This Application (10/092972)	U.S. Patent No. 6487661B2
Claims 1-10	1-10, 18, 19

Claims 11-15	11-15

Exemplary Claim 1 in "972	Exemplary Claim 1 in "661
A method of authenticating a pair of correspondents A, B to permit exchange of information there between, each of said correspondents having a respective private key a, b and a public key Pa, Pb derived from a generator α and respective ones of said private keys a, b, said method including the steps of i) a first of said correspondents A selecting a firs random integer x and exponentiating a function f(a) including said generator to a power $g^{(x)}$ to provide a a first exponentiated function $f(\alpha)^{g(x)}$; ii) said first correspondent A forwarding to a second correspondent B a message including said first exponentiated function $f(\alpha)^{g(x)}$; iii) said correspondent B selecting a	A method of authenticating a pair of correspondents A, B in a public key data communication system to permit exchange of information there between over a communication channel, each of said correspondents having a respective private key a, b and a public key p.sub.A, p.sub.B derived from a generator .alpha. and respective ones of said private keys a, b, said method including the steps of: i) a first of said correspondents A selecting a first random integer x and exponentiating a first function f(.alpha.) including said generator to a power g(x) to provide a first exponentiated function f(.alpha.).sup.g(x) ; ii) said first correspondent A forwarding to a second correspondent B a message including said first exponentiated function

second random integer y and exponentiating a function f(α) including said generator to a power g(y) to provide a second exponentiated function $f(\alpha)^{g(y)}$; iv) said second correspondent B constructing a session key K from information made public by said first correspondent A and information that is private to said second correspondent B, said session key K also being constructible by said first correspondent A for information made public by B and information that is private to said first correspondent A; v) said second correspondent B generating a value h of a function F(δ,K) 2 1 where F(δ,K) denotes a cryptographic function applied conjointly to δ and K and where δ is a subset of the public information provided by B thereby to bind the values of δ and K; vi) said second of said correspondents B	f(.alpha.).sup.g(x) ; iii) said correspondent B selecting a second random integer y and exponentiating a second function f'(.alpha.) including said generator to a power g(y) to provide a second exponentiated function f'(.alpha.).sup.g(y) ; iv) said second correspondent B constructing a session key K from information made public by said first correspondent A including said public key p.sub.A, and information that is private to said second correspondent B, said session key K also being constructible by said first correspondent A from information made public by said second correspondent B including said public key p.sub.B, and information that is private to said first correspondent A; v) said second correspondent B generating a value h of a function F[.pi., K] where F[.pi., K] denotes a

forwarding a message to said first correspondent A including said second exponential function $f(\alpha)^{g(y)}$ and said value h of said cryptographic function F(δ,K); vii) said first correspondent receiving said message and computing a session key K' from information made public by said second correspondent B and private to said first correspondent A; viii) said first correspondent A computing a value h' of a cryptographic function F(δ,K'); and ix) comparing said values obtained from said cryptographic functions F to confirm their correspondence	cryptographic function F applied conjointly to .pi. and K to bind the values of .pi. to K and where .pi. is obtained from said information made public by said second correspondent B to permit construction of said session key K; vi) said second of said correspondents B forwarding a message to said first correspondent A including said second exponentiated function f'(.alpha.).sup.g(y) and said value h of said cryptographic function F[.pi., K]; vii) said first correspondent receiving said message and computing a session key K' from said information made public by said second correspondent B and private to said first correspondent A; viii) said first correspondent A computing a value h' by application of a cryptographic function F to .pi. and K'; and ix) comparing said values obtained from said application of said cryptographic functions F to confirm their correspondence.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100